什么是UNIX mbox (邮箱)格式？

Contents

[Introduction](#)
[什么是UNIX mbox (邮箱)格式？](#)

Introduction

本文描述Unix邮箱(mbox)格式，并且如何在Cisco电子邮件安全工具(ESA)上关连使用。

什么是UNIX mbox (邮箱)格式？

UNIX AsyncOS使用mbox格式，当归档时消息并且登陆消息过滤器log()动作。“档案消息”是Ironport Anit垃圾邮件(IPAS)，抗病毒(Sophos和McAfee)，先进的Malware保护(AMP)和Graymail的其他配置选项在ESA。

Mbox格式是能包含零个的一种ASCII格式化的(即不二进制)文件格式或更多邮件消息。消息在mbox文件被连接，并且可以分开被撬起根据在文件的特定字符串。因为他们调用在RFC 2821兼容邮件网关之间，此格式是完全相同和消息。

每个消息以mbox格式从从字符串开始“”的线路开始(ASCII字符F、r、o、m和空间)。“从”线路由几个更多字段跟随：包发送方、日期和(可选地)更多数据。

在以后的第一个字段“从”字符串是消息的包发送方。从属在哪个应用程序创建mbox文件，包发送方也许是存在，当实际邮箱或它也许是另一个字符或字符串。通常，您将发现“-” (单个字符破折号)替换包发送方，如果实际包发送方不是可用或没已知。ESA插入的日期字段是以标准的UNIX asctime()格式并且总是长度24个字符。在非AsyncOS实施写的一些mbox文件，详细信息跟随日期标记。这三个字段由一个空格分隔。

这是一个mbox文件的示例与单个消息的在它：

```
From Adam@Outside.COM Sun Oct 17 12:03:20 2004
Received: from mail.outside.com (192.35.195.200)
by smtp.alpha.com with ESMTP; 17 Oct 2004 12:03:20 -0700
X-IronPort-AV: i="3.85,147,1094454000";
v="EICAR-AV-Test'0'v";
d="scan'208"; a="86:adNrHT37924848"
X-IronPort-RCPT-TO: alan@mail.example.com
From: Adam@Outside.COM
To: Alan Alpha <Alan@mail.example.COM>
Subject: Exercise 7a Anti-Virus Scanning
Reply-To: Adam Alpha <adam@outside.com>
Date: Sun, 17 Oct 2004 12:02:39 -0700
MIME-version: 1.0
Content-type: multipart/mixed; boundary="IronPort"

--IronPort
Content-type: text/plain; format=flowed; charset=us-ascii
Content-transfer-encoding: 7bit
```

```
Blah blah blah blah blah
Blah blah blah blah blah
Blah blah blah blah blah
...
--IronPort
Content-type: text/plain
Content-transfer-encoding: 7bit
Content-disposition: inline

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*">X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

--IronPort--
```

当mbox格式化的文件解析时，不读许多语义到“从”分离消息的线路是理想的。由于许多不同的工具写mbox文件，有在这些线路上的严重的变化。然而，“从”线路可能总是用于，当消息分隔符线路为了可靠表明一个新的消息在mbox文件开始了。总计，有大约字符串的20种已知格式在以后“从”消息分隔符，通常使非常困难解析他们。

在“从”线路是一个电子邮件消息以RFC 2822格式后，当一系列的消息正文报头跟随由另外的消息正文内容跟随的空行。

为了保证消息适当地被分离，从字符串请开始“”的线路由单个总是加在前面“>”。mbox从“>From”不同地开始的文件处理线路多种不同的变形。在写mbox文件应用程序的早期实施，未引述这些线路他们自己。AsyncOS日志文件永远将加在前面“>”对从一个或更多“>”字符请开始跟随“从”的线路。

这是包含一个消息有线路请包含开始的字符串“”，“>From”和“>>>>From”在它mbox文件的示例：

```
From jtrumbo@example1.com Sun Dec 12 12:27:33 2004
X-IronPort-RCPT-TO: trumbo@example1.com
From: jtrumbo@example1.com
To: trumbo@example2.com
Subject: Quote this, if you dare
Date: Sun, 12 Dec 2004 12:28:00 -0700

The following line is just From
>From A From Line

The following line has quoted >From
>>From A >From Line

The following line has many >>>>From
>>>>>From This line has 4 > characters before From

And this is the last line
```

一个消息的末端在mbox格式文件的由空行传统上发信号。然而，这总是不存在(虽然AsyncOS放置它那里)。当mbox格式文件解析时，您应该发信号消息的末端由一个新的消息的开始(请删除空行，如果一个存在)或在文件以前。

另一变量以要求在信息标题内的一个“内容长度”字段将发信号的消息的长度mbox格式。该格式没有从”线路引述使用“。AsyncOS不使用此格式，并且不插入内容长度字段。